



Managing Information Security Problems



Clarence Hoop
Chief, Plans, Policy & Integration
Division

DIS^w CISS

Phone: (703) 681-7988

hoopc@ncr.disa.mil

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 01011996	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Managing Information Security Problems		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) DISA		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Document Classification unclassified		Classification of SF298 unclassified
Classification of Abstract unclassified		Limitation of Abstract unlimited
Number of Pages 34		

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 1/1/96	3. REPORT TYPE AND DATES COVERED Briefing	
4. TITLE AND SUBTITLE Managing Information Security Problems			5. FUNDING NUMBERS	
6. AUTHOR(S) Clarence Hoop				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) This DISA Briefing discusses the topic of Managing Information Security Problems. The areas the briefing covers are: The operational environment; what are some of the problems encountered; what is happening in the community today and what are the community plans for the future. It addresses the issues of insider threat, external threat, how to cope with the threats, use of firewalls and the Defense in Depth strategy.				
14. SUBJECT TERMS IA			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT None	



Presentation Outline

What is the Operational Environment?

What are some of the problems encountered?

What are we doing today?

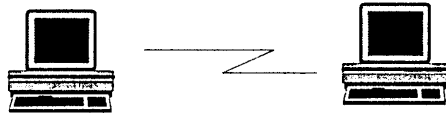
What do we plan for tomorrow?



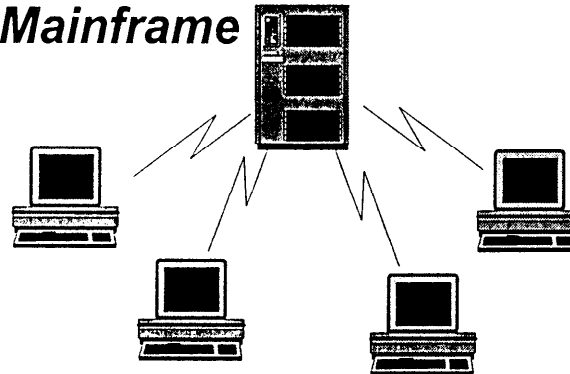


Technology Revolution

Point-to-Point



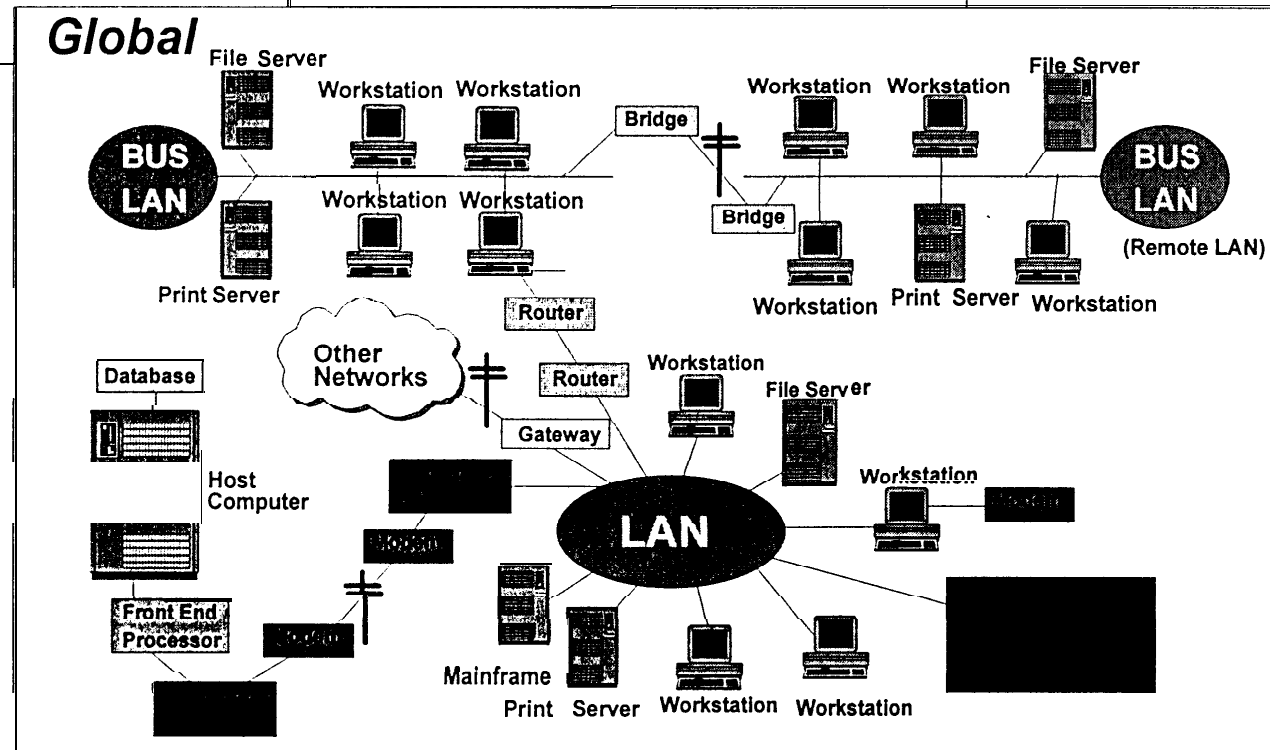
Mainframe



DISN

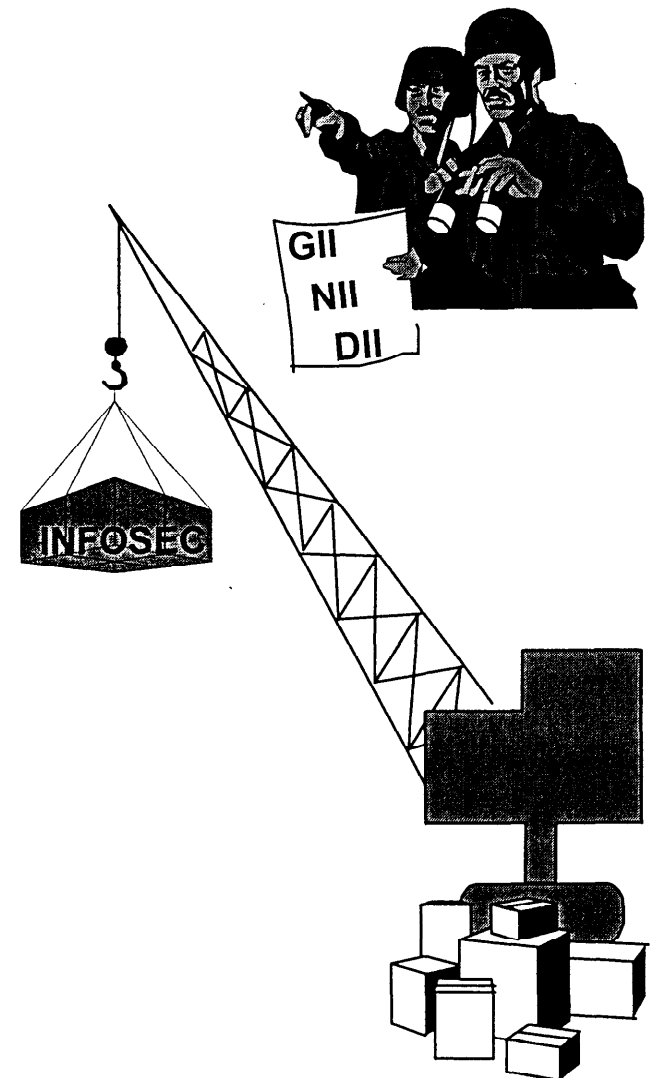
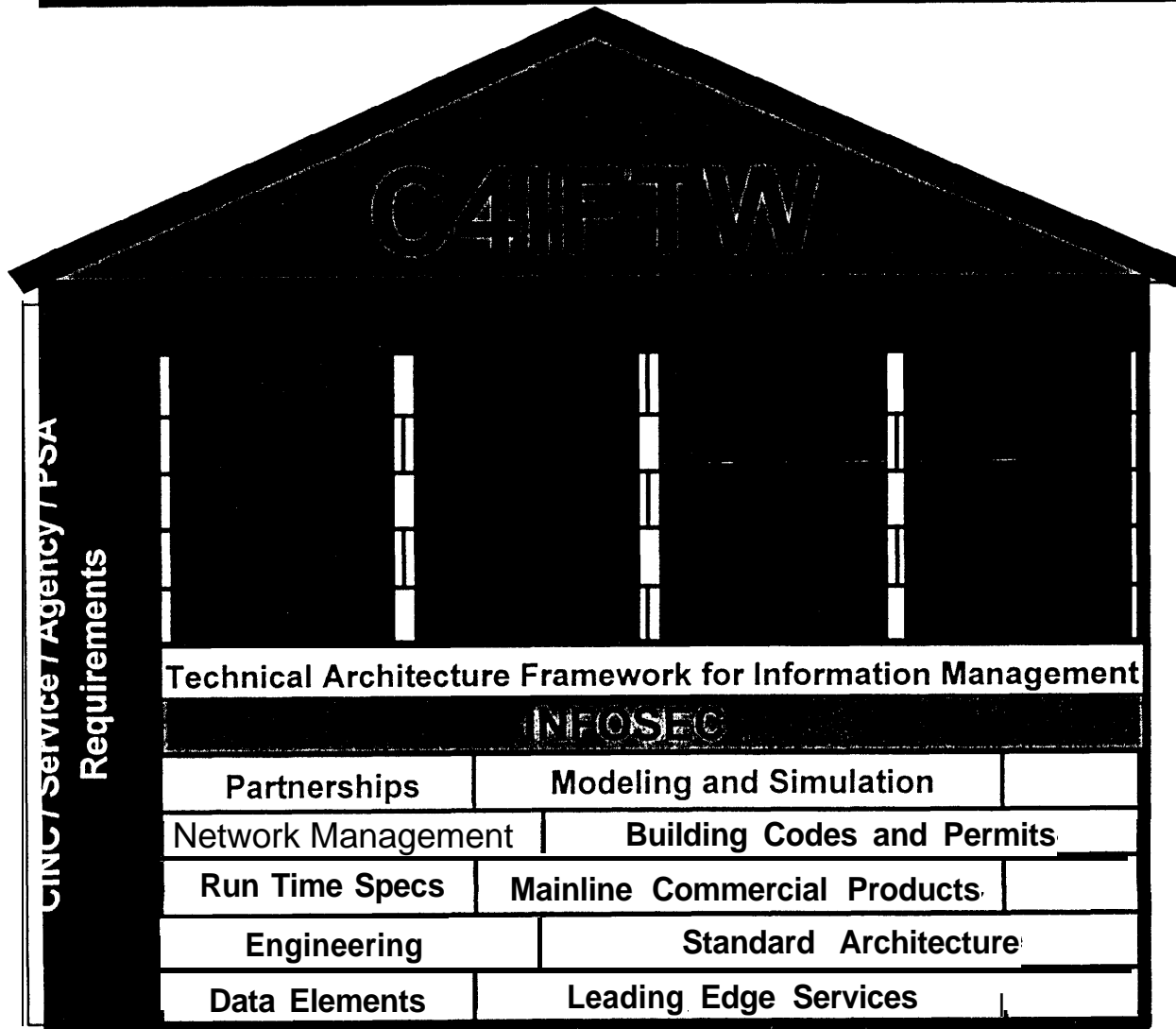
- ✓ Transmission
- ✓ Command & Control
- ✓ Messaging
- ✓ Combat Support

Global





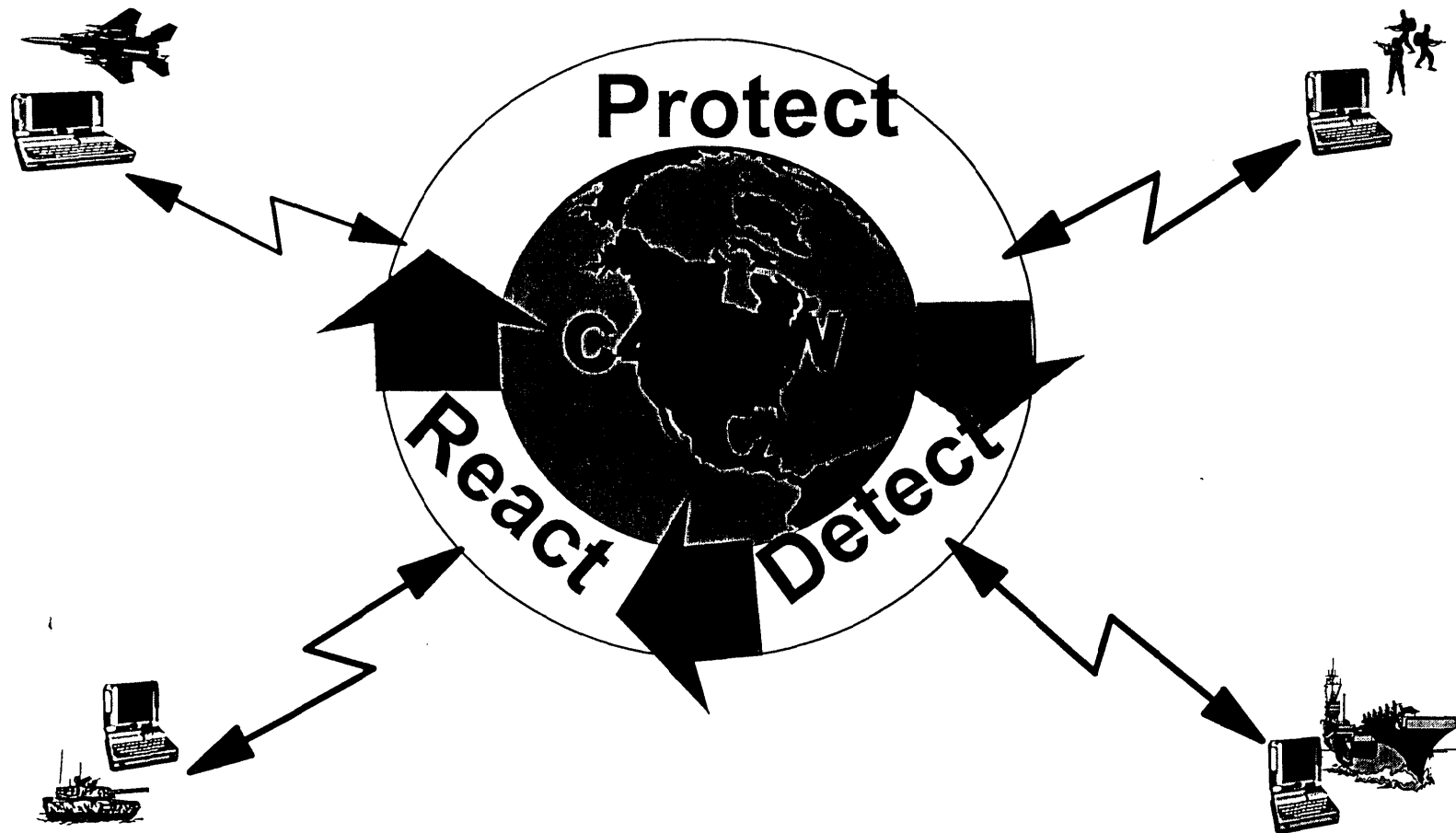
C4I for the Warrior



DISA: ARCHITECT OF THE FUTURE



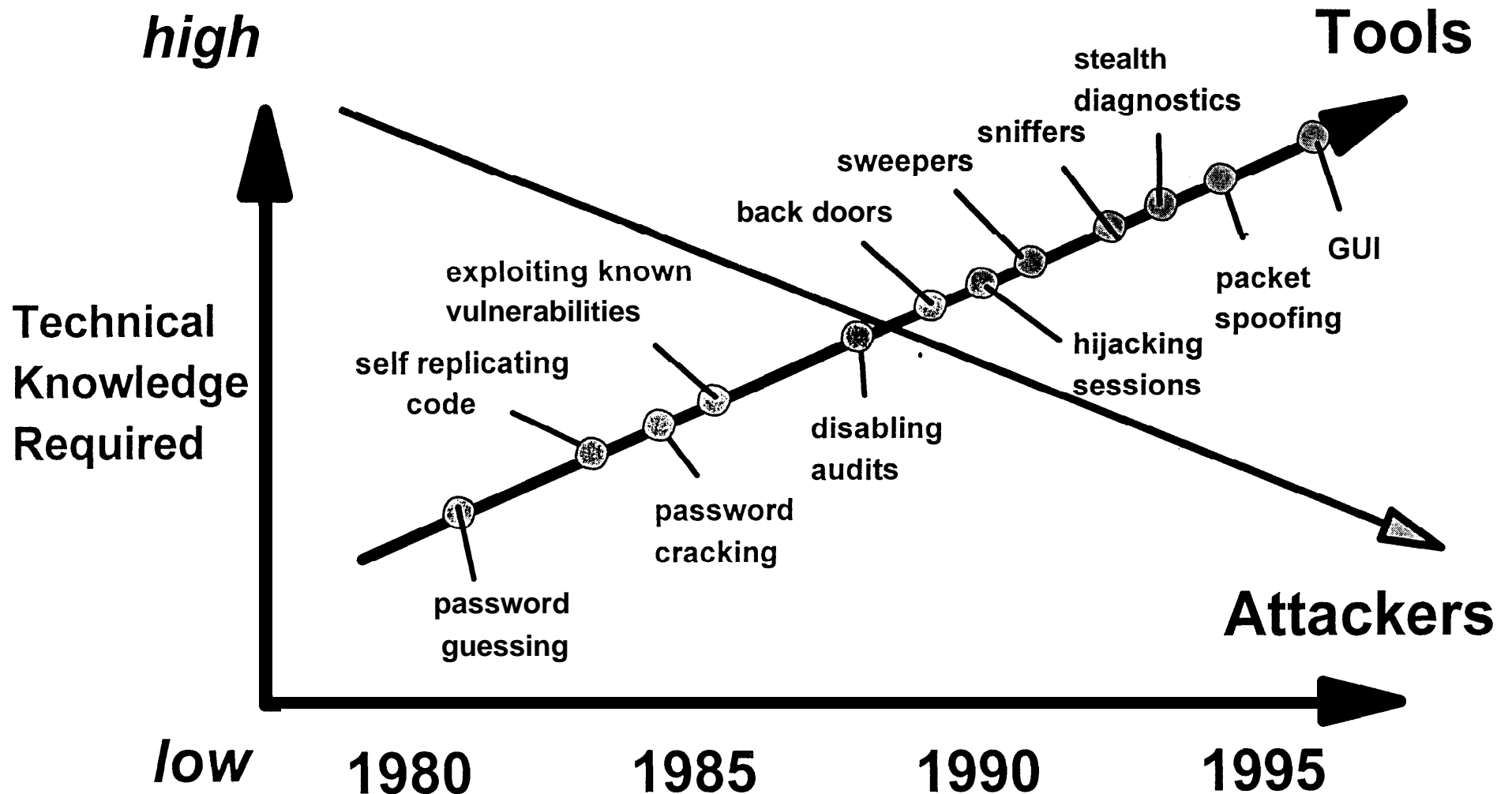
DISA INFOSEC STRATEGY: Supporting the DISA Mission



Defend the DII: Anywhere, Anytime, Any Mission

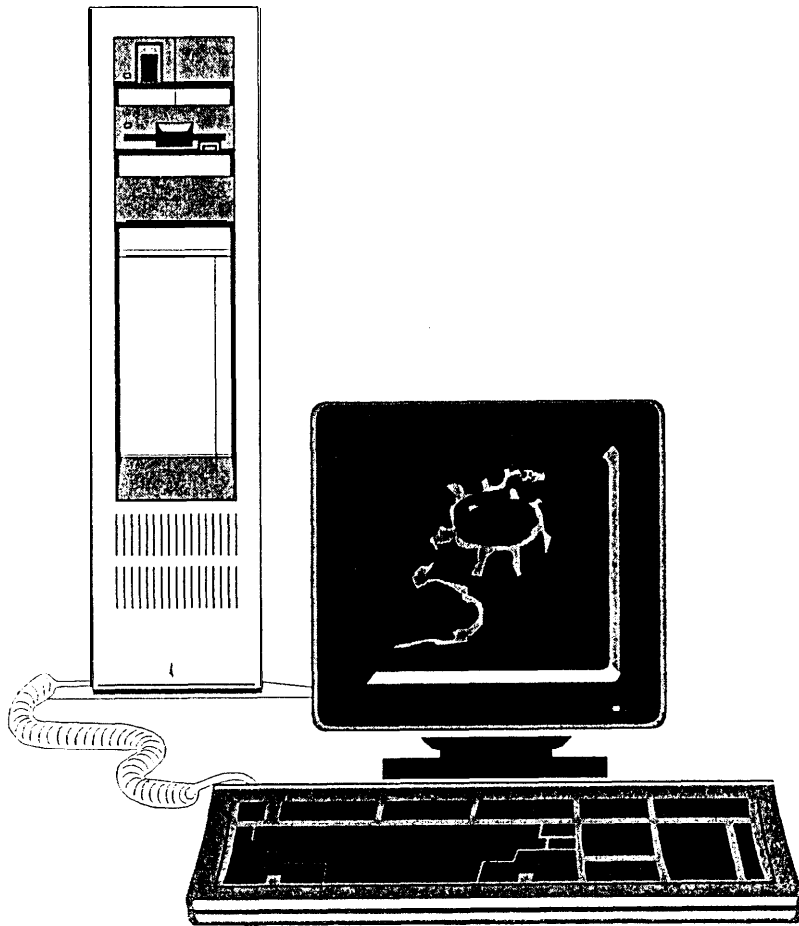


Intruder Technical Knowledge





Intruders Have Been Observed



Destroying data

Destroying software

Modifying Data

Modifying software

Stealing data

Stealing software

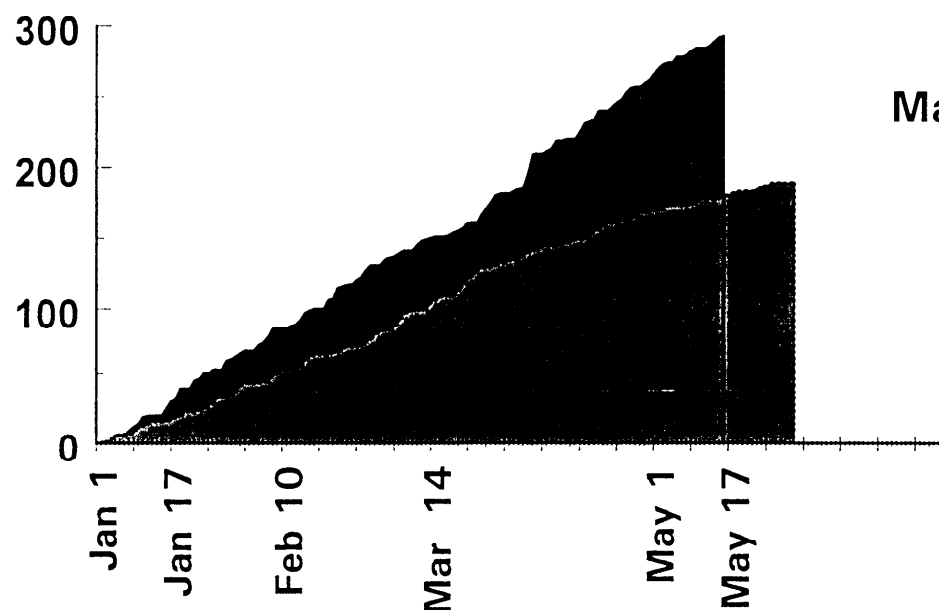
Shutting down
hosts/networks

Using **DoD** systems
as launch points



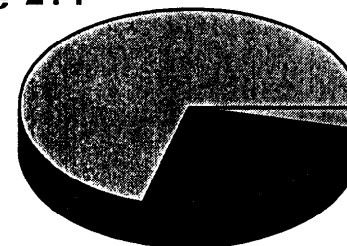
Incidents Reported to DISA/ASSIST

Reported Incidents



■ 1996 - (303) ■ 1995 - (180)

Malicious Code 214



Other 11

Intrusions 78

1996 Incident Breakdown

As of 2400 hrs 23 May 96



What do we see at ASSIST?

Tools & Techniques

- Telnet/ftp
- Password Files/tftp/Crack
- Sendmail/smtp
- Sweepers
- finger
- Sniffer
- r* commands
- IP spoofing
- Rootkit





What do we see at ASSIST?

Virus Contenders

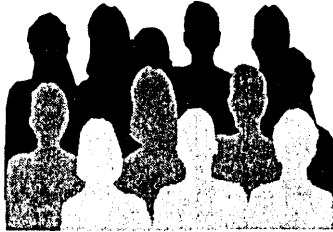


- Word Macro Virus
- Monkey
- Form
- BUPT
- AntiExe
- Jack the Ripper



Where do they get those toys?

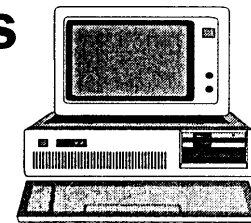
Newsgroups



FTP Sites

WEB Pages

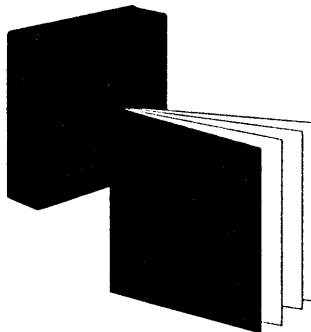
BBSs



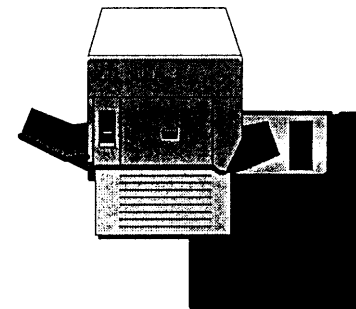
Books

Magazines

Ezines



Trade





An Example of DoD Functions Affected

Composite Material Research	Mathematical Simulations	Military Health Systems
Structural Research on Ships/Planes	Supply and Maintenance Support System	High Performance Computing Systems
Personnel Management Services	Master Clock for 1/4 of the WORLD	Supercomputer Research Network
Ballistic Weapons Research	Command Tasker System	Artificial Intelligence Research
R&D on Health Sciences	Mail Hub for Post-wide Electronic Mail	Knowledge Based Simulation
R&D on Ocean Sciences	Finance Databases	Applied Research in Photonic Technology
Inventory and Property Accounting	Procurement	Force Level Execution
Organizational Service Training	Scientific Modeling for Battlefield Environment	Battle Management Decision Aids (Presentation)
Payroll and Business Support	C3 Development	
Finite Element Analysis of Submarine Structures	Ocean Surveillance	



INFOSEC Functions





VISION & STRATEGY FOR DEFENSIVE INFORMATION WARFARE

**Establish Teaming Relationships, leverage work
Cost effective fixes for critical vulnerabilities,
Establish IW-D Command & Control Center,
Provide Standardized Certification/
Accreditation of DII,
&
Reflect IW-D process in
every program**

**CINC. Service,
& Agency IW
Program Plans**

**DISA IW
Program**

DISN

DMS

GCOS

**Defense Mega
Centers**

EG/EDI

**Other
Programs**



DISA's Multi-Disciplined Security Process

**INFOSEC Engineering,
Integration
& DOD MLS Program**

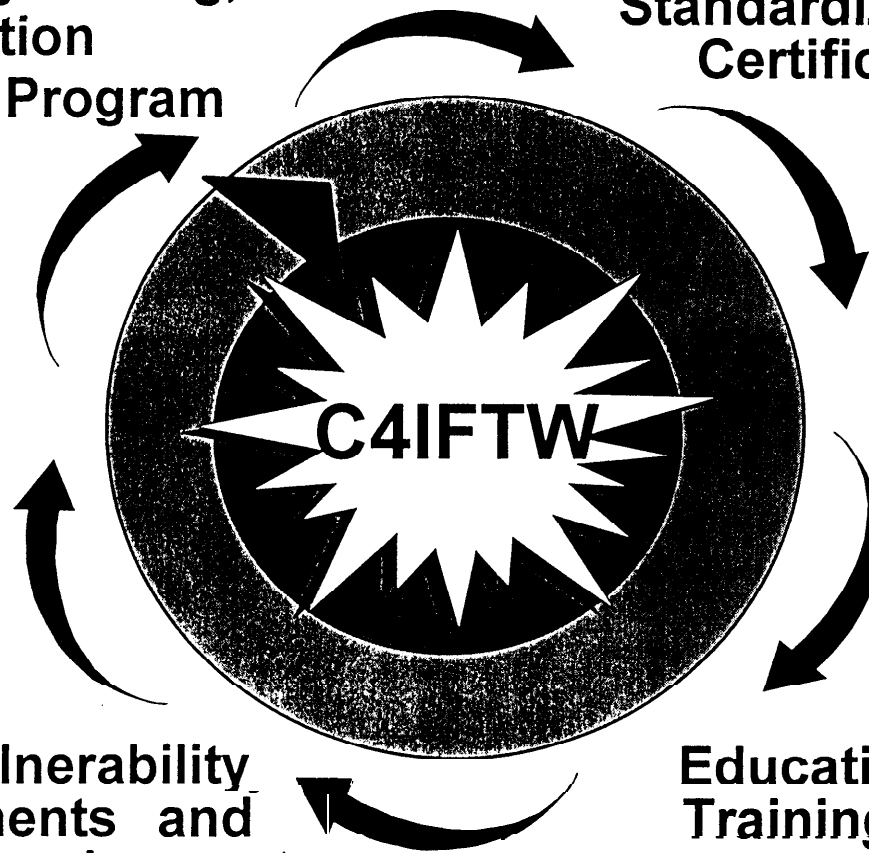
**Standardized DOD
Certification**

**Integrated
Operations,
Monitoring,
and VAAP**

**Policy &
Plans**

**Threat/Vulnerability
Assessments and
Tool Development**

**Education,
Training &
Awareness**



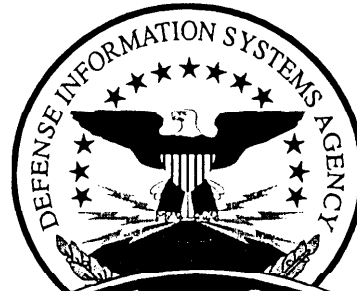
INFOSEC Technical Services Contract



Collaborative Work Environment

Defend the DII

*All Source
Intelligence
Assessments*



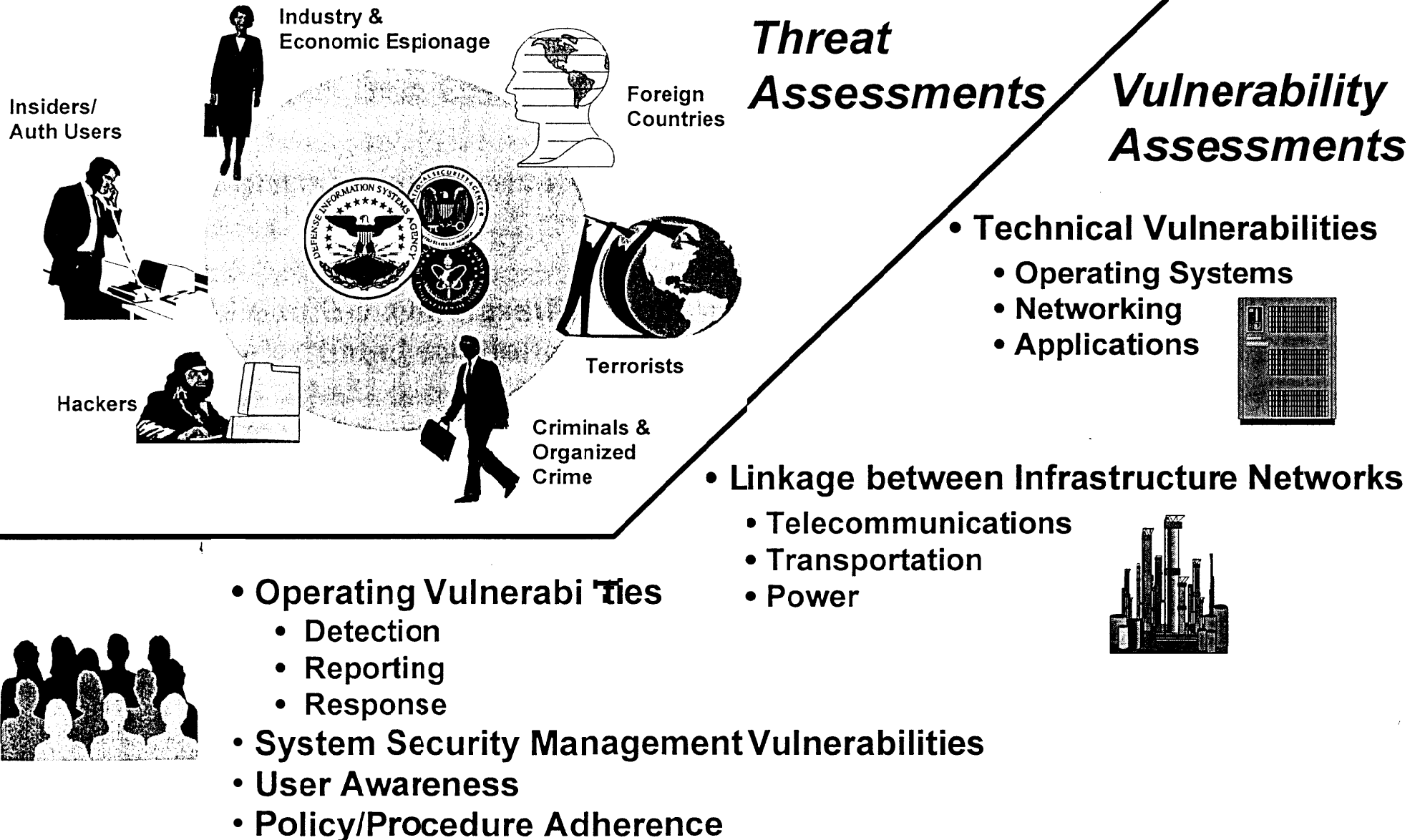
*INFOSEC Product
Development &
Integration*



FOCUS: Get INFOSEC Products to the Warfighter!



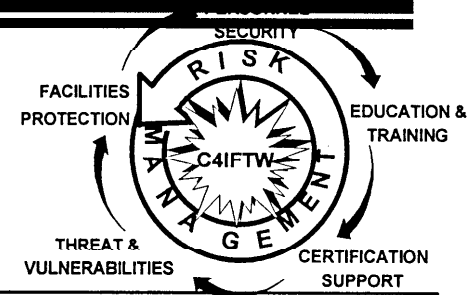
Threat & Vulnerability



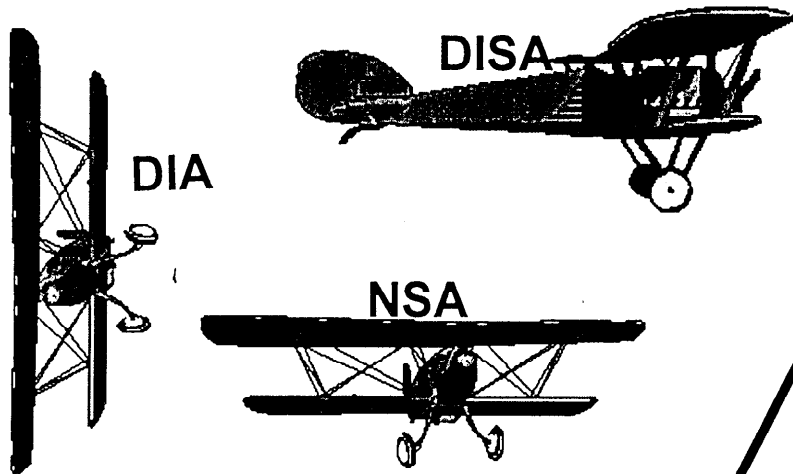


Standard Certification Process

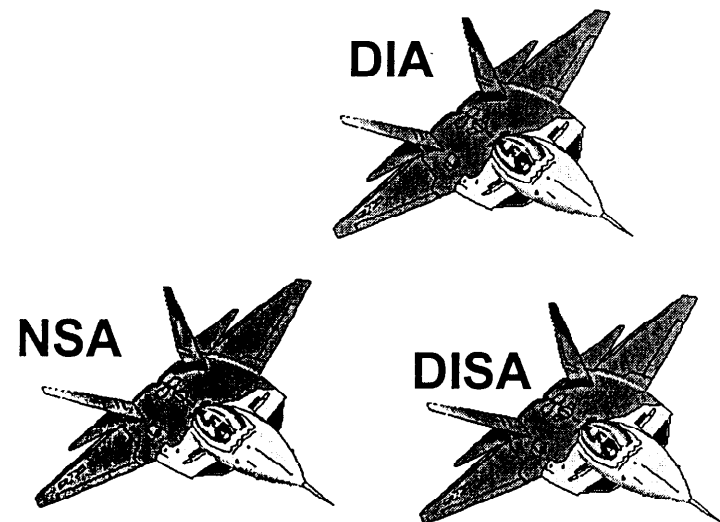
DITSCAP: DOD Information Technology Security Certification and Accreditation Process



Current: System-Centric



**DITSCAP:
Infrastructure-Centric**



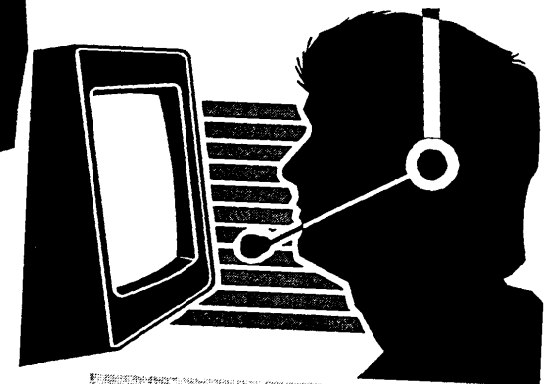


Current Operations

Integrated Operations Center



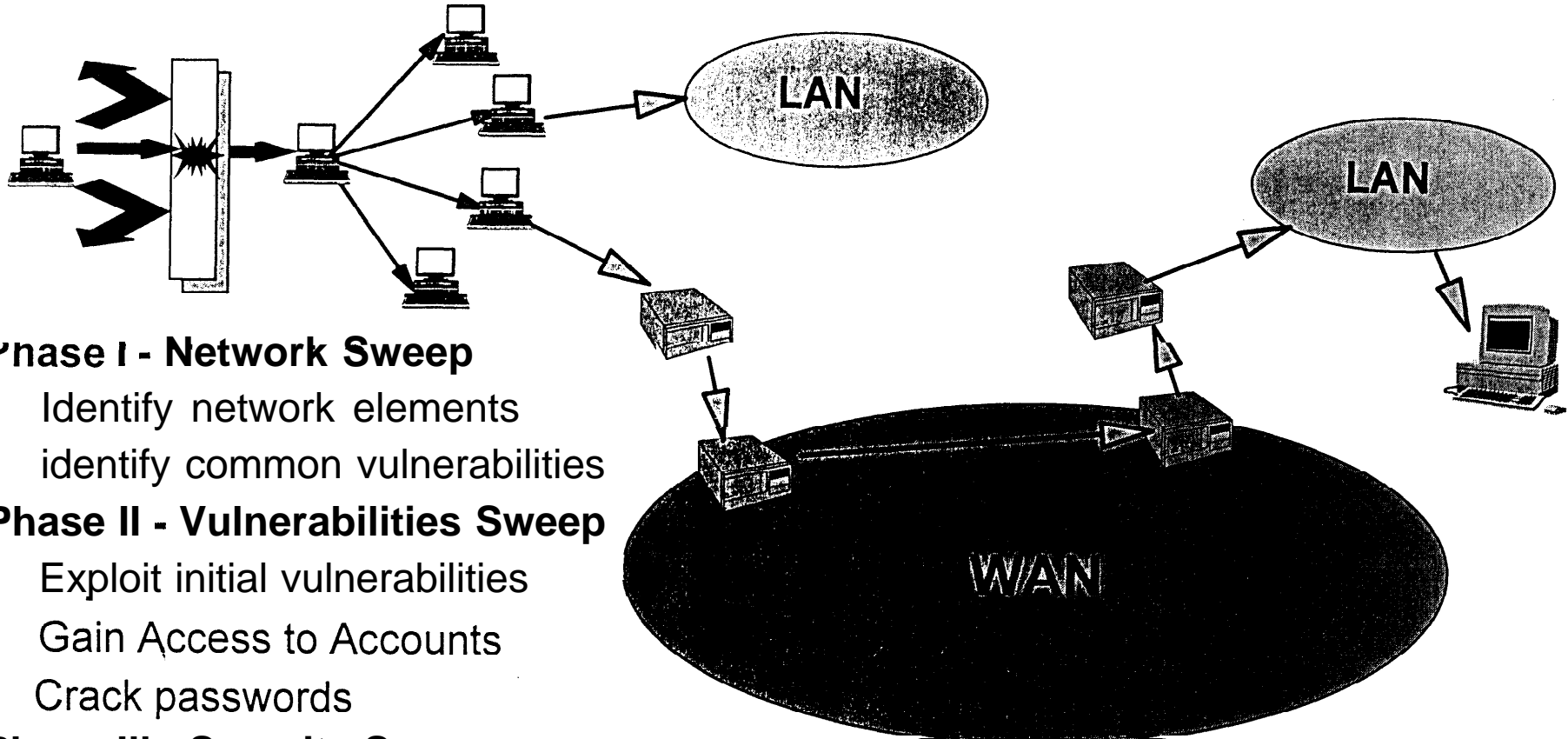
Network Ops



ASSIST



Vulnerability Assessments



Phase I - Network Sweep

Identify network elements

identify common vulnerabilities

Phase II - Vulnerabilities Sweep

Exploit initial vulnerabilities

Gain Access to Accounts

Crack passwords

Phase III - Security Sweep

Attain Greater Access

install Trojan Horses

Exploit trusted relationships

Exploit network vulnerabilities

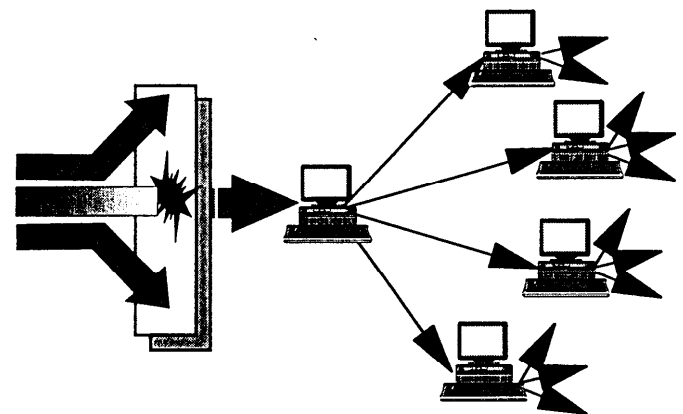
Current Focus on UNIX
and TCP/IP



Vulnerability Analysis & Assistance Program Findings

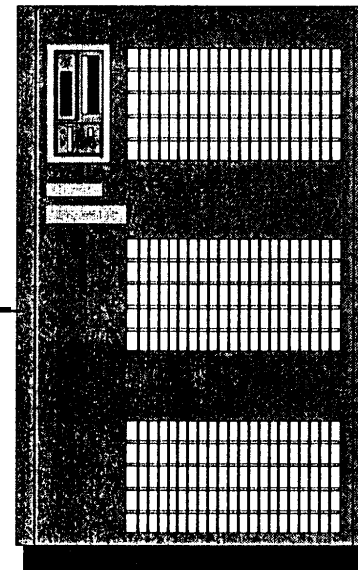
Based on 77 assessments on 38,726 Host Computers:

- . 4.4% of DOD unclassified computers tested have “easily” exploitable front doors**
- . 65% - 89% of DOD unclassified computers tested can be further penetrated by network trusted relationships (not an indication of overall health of DII)**
- . 96% of VAAP penetrations undetected by host administrators and users**
- . 73% of detected penetrations go unreported**





Defense in Depth: Avoid a Single Point of Failure

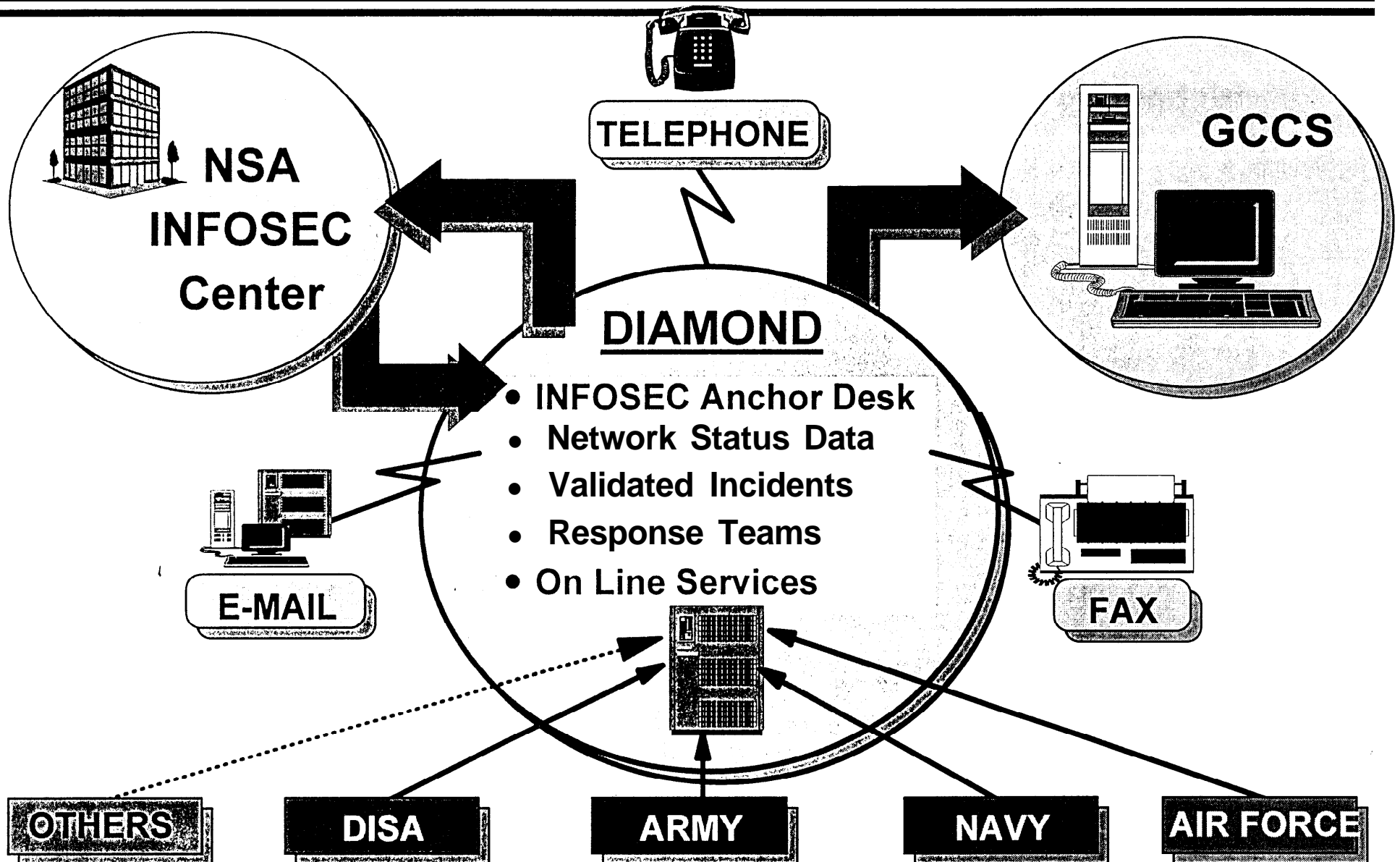


Connecting Lan: Do the
Hosts pass the Vulnerability
Sweep?


Firewalls: Do they
meet the security
and operational
requirements?



Defense Intrusion Analysis and Monitoring Desk (DIAMOND)

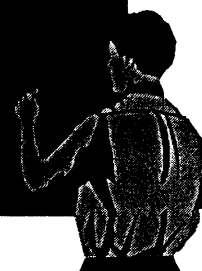


GCC
RCCs
DMCs
DCTF
NIPRNet Gateways



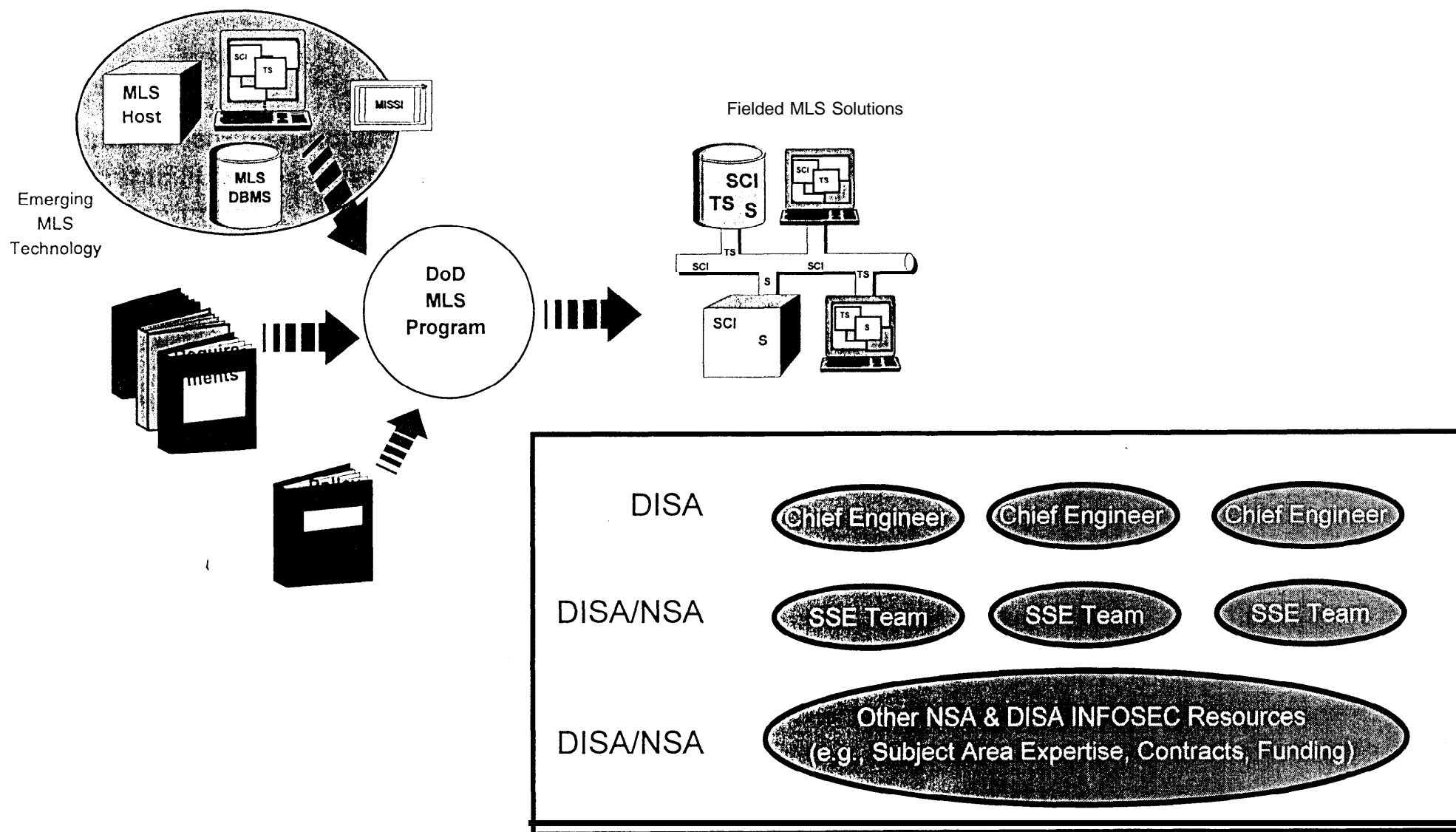
Gold Report

Analysis





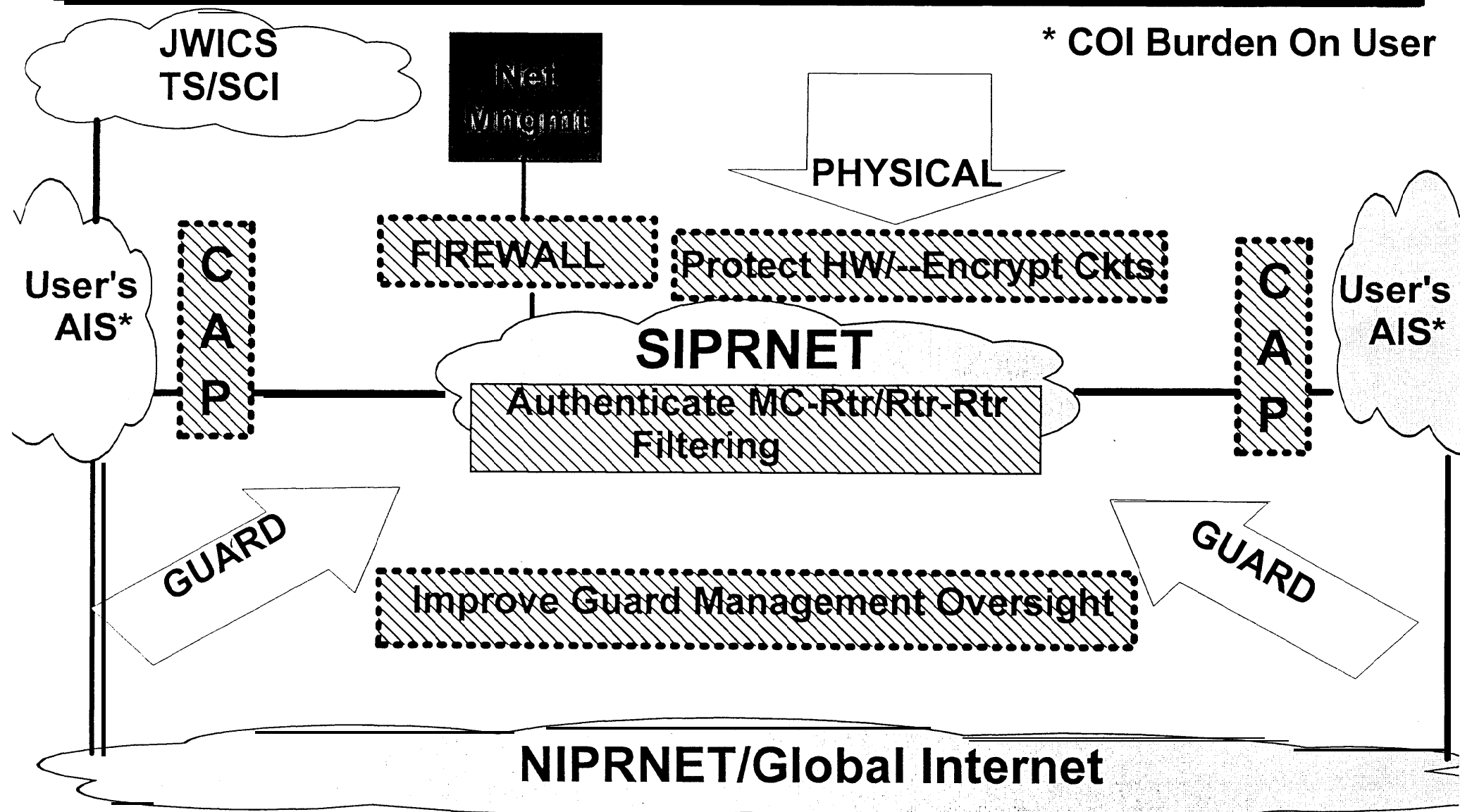
INFOSEC Engineering & DOD MLS Program





Network Protection

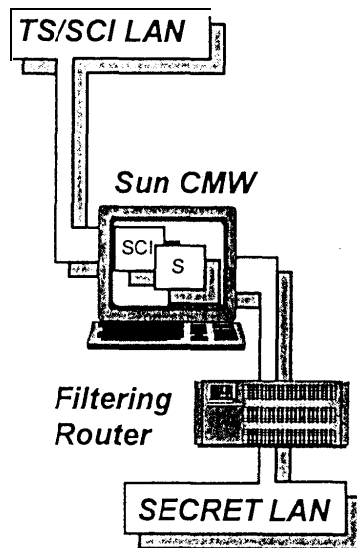
* COI Burden On User



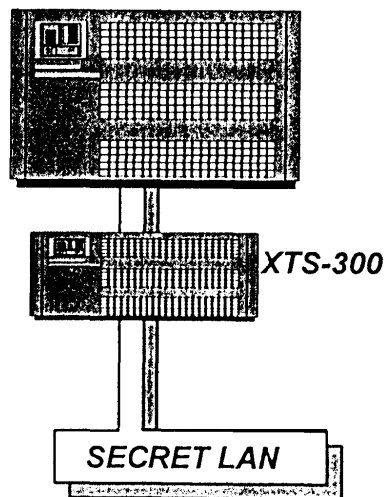


Current Security Products

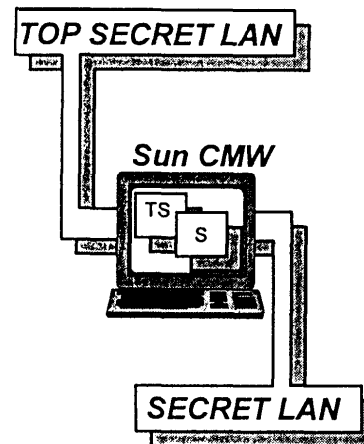
Ops/Intel Interface



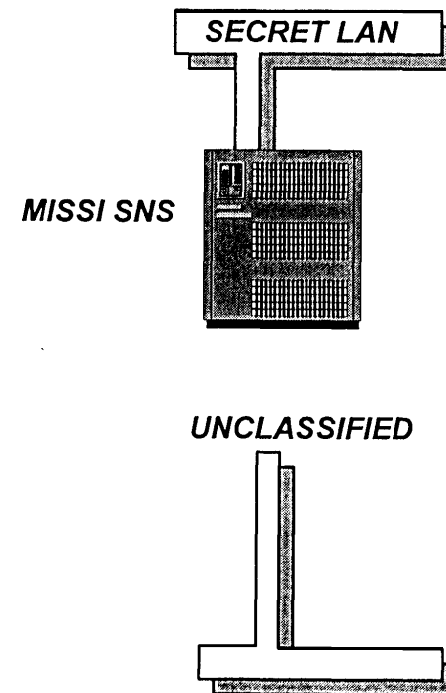
C2 Guard



Two-Level Workstation

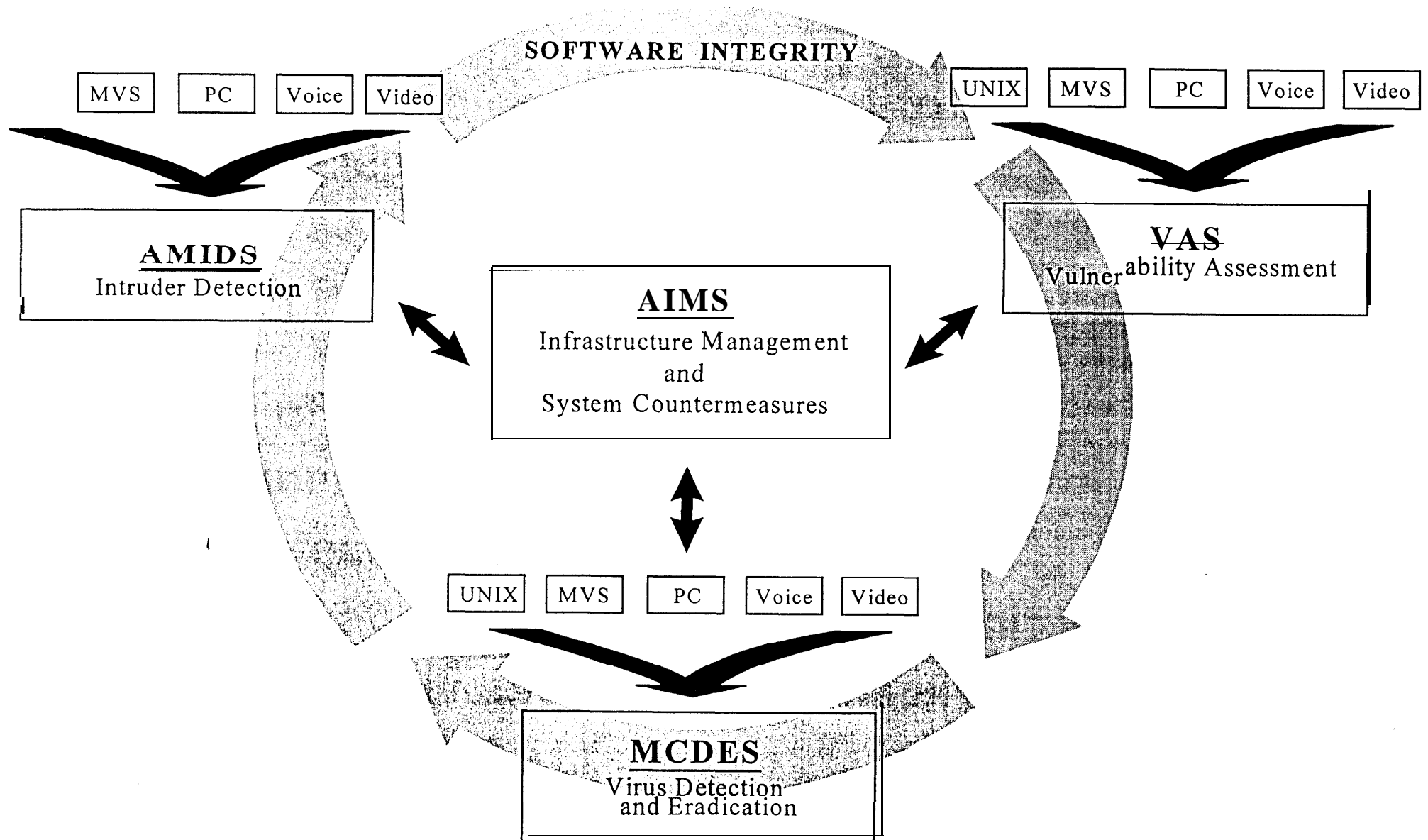


Standard Mail Guard



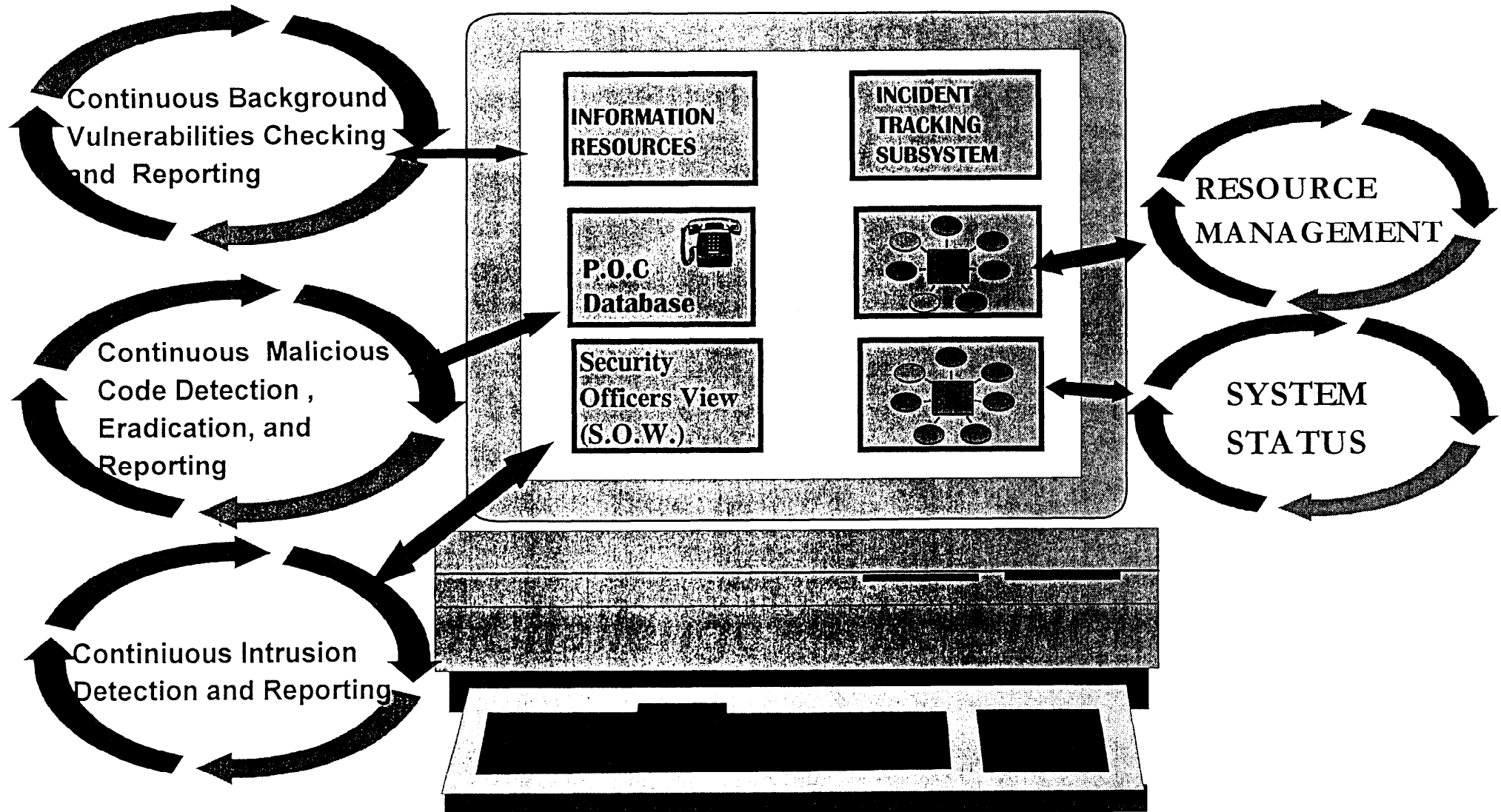


Tools: How Do they Fit Together



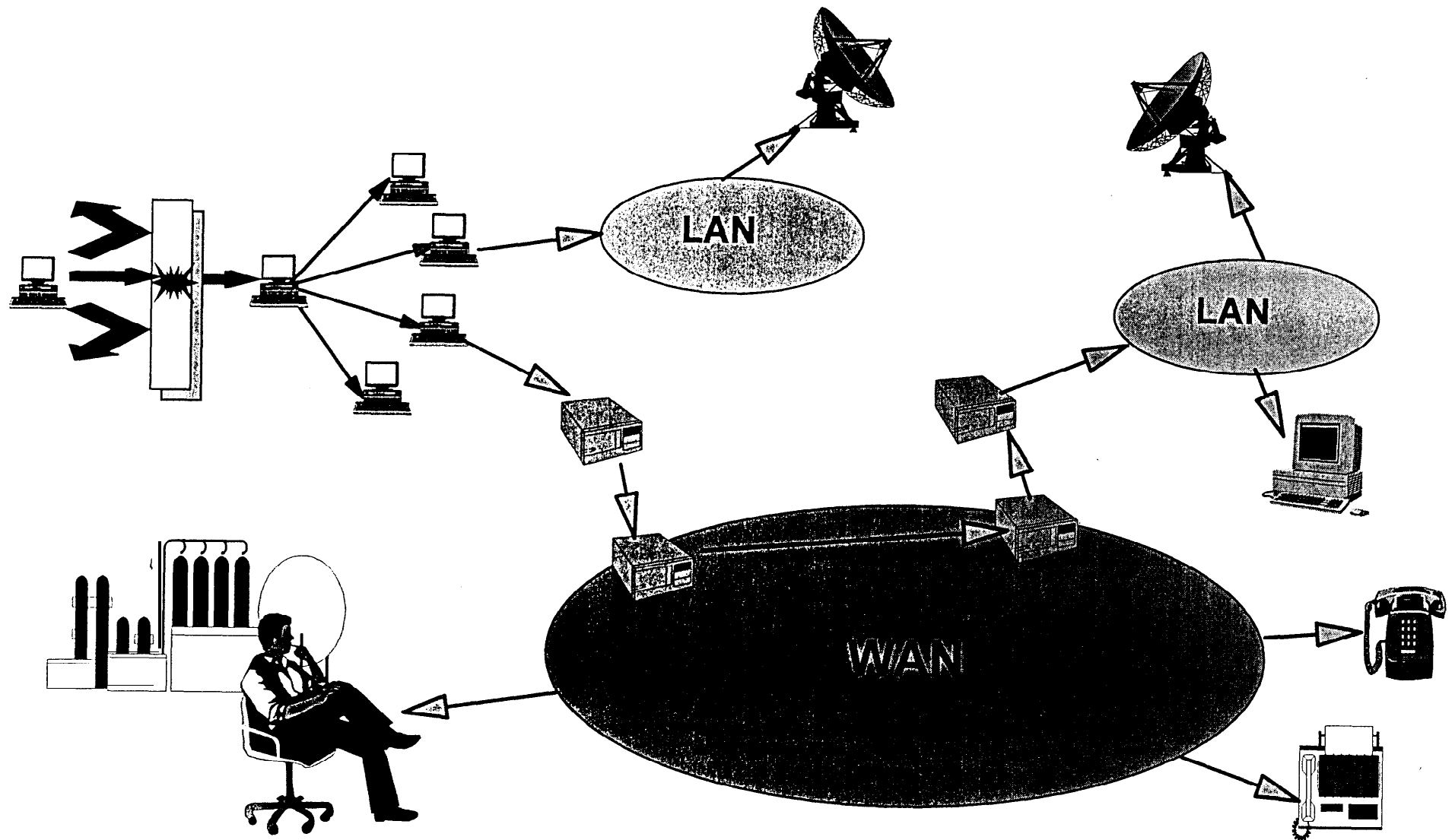


Automated Infrastructure Management System





Managing Vulnerability Assessments: Integrated Tools & Red Teams

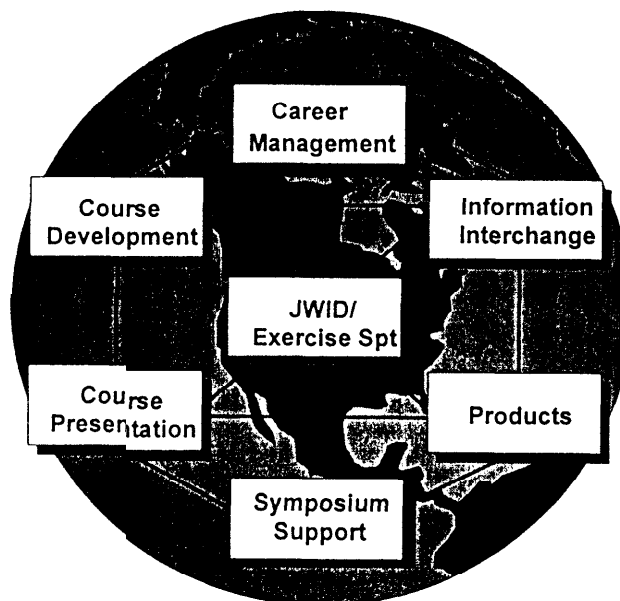
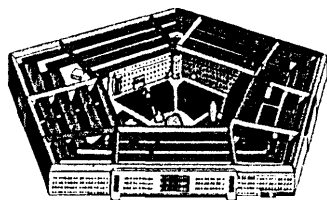




INFOSEC Education, Training & Awareness

Mission:

- Courseware Development and Delivery
- INFOSEC Awareness Products
- INFOSEC Professional Development



Army



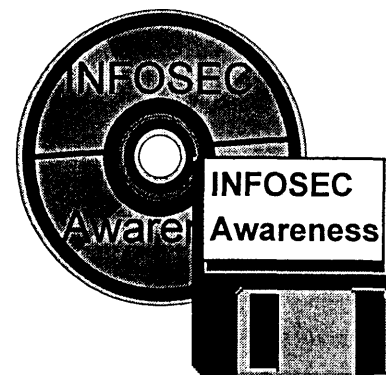
Navy



Air Force



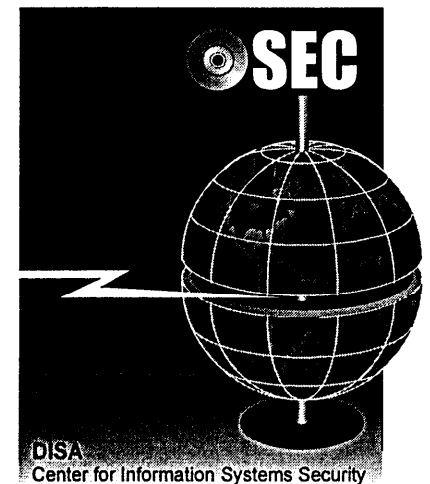
Marines





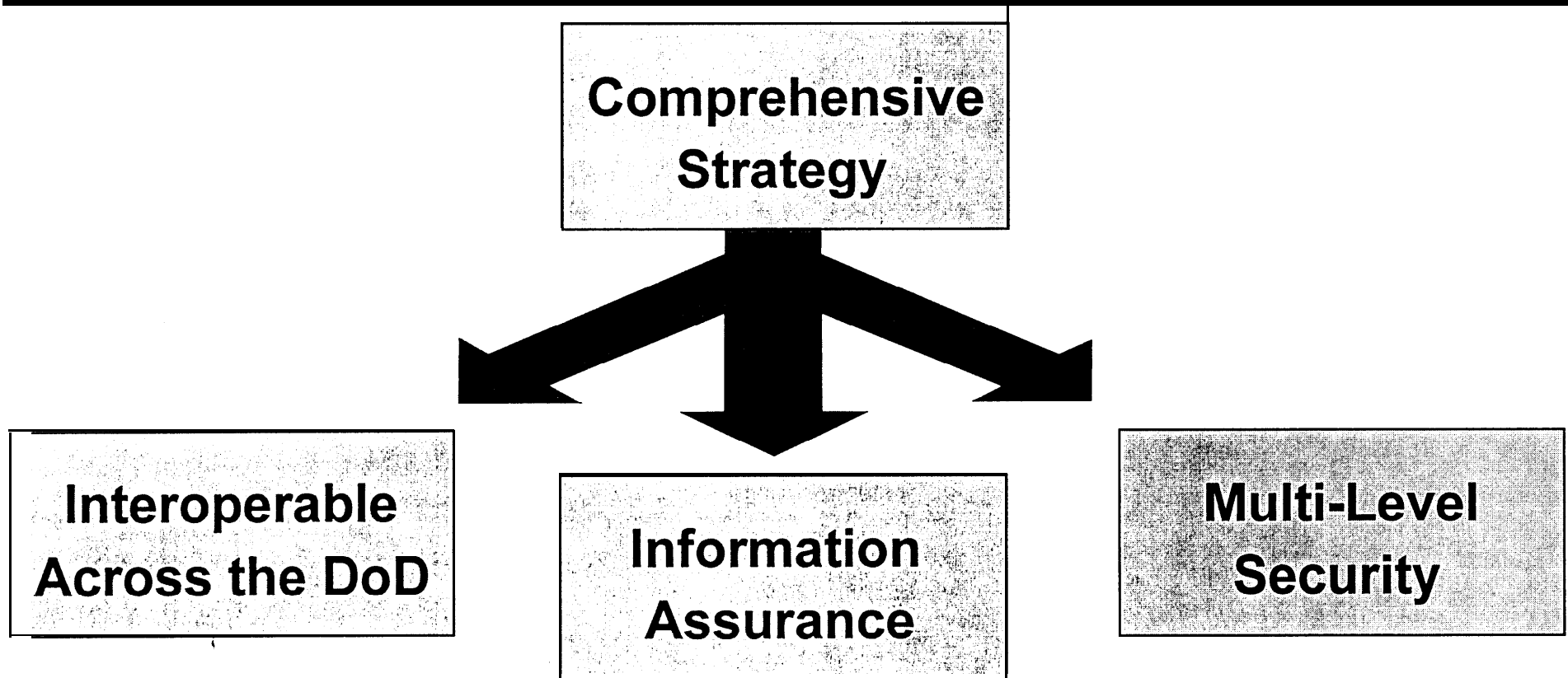
INFOSEC Technical Services Contract

- Quick reaction contract support to DOD & other Federal Departments/Agencies
- Three Contractor Teams
- Areas of Support Include:
 - Engineering
 - Architecture
 - Certification, evaluation and accreditation
 - Vulnerability assessment tools and techniques
 - Training and Awareness





Summary: The Way Ahead



Multifaceted Challenge - - No SINGLE Solution